

F5 BIG-IP & BIG-IQ Vulnerabilities

Critical Bug Allowing Remote Code Execution

https://www.f5.com/services/support/March2021_Vulnerabilities
CVEs: [CVE-2021-22986](#), [CVE-2021-22987](#), [CVE-2021-22991](#), [CVE-2021-22992](#)

The 2 most critical vulnerabilities allow a remote attacker with access to the user interface (or REST API via the user interface) to gain full control of the system and execute arbitrary system commands, create or delete files, and disable services. The most critical is unauthenticated. Exploitation can lead to complete system compromise. The U.S. Cybersecurity and Infrastructure Agency (CISA) has urged companies using BIG-IP and BIG-IQ to fix the critical F5 flaws.

Background

These are `in the wild` vulnerabilities for existing software - refer to versions listed by F5 to see if you are impacted based on the versions you may be running. Details for the 2 most critical vulnerabilities can be found in the big tables on these articles:-
<https://support.f5.com/csp/article/K18132488>

<https://support.f5.com/csp/article/K03009991>

Latest Developments

March 20, 2021: On March 20, multiple stories reported the F5 vulnerabilities under `active attack`. FortiGuard IPS protects against 3 of the 4 critical CVEs identified (the 4th being 22987 which requires authentication). FortiGuard Labs Threat Signal Report is available from:
<https://www.fortiguard.com/threat-signal-report/3891>


March 10, 2021: F5 announced several vulnerabilities and strongly urged customers to upgrade:
https://www.f5.com/services/support/March2021_Vulnerabilities

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

AV


Detects known malware related to the Outbreak



FortiADC


IPS

Detects and blocks attack attempts leveraging the vulnerability




FortiADC

DB 18.044




FortiGate

DB 18.044




FortiNDR

DB 18.044



FortiProxy

DB 18.044




FortiSASE

DB 18.044


DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:


IOC




FortiAnalyzer



FortiSOCaaS

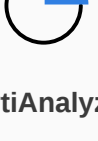


FortiSIEM



FortiSOAR

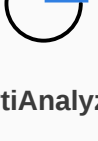
Outbreak Detection



FortiAnalyzer


DB 1.00033

Threat Hunting



FortiAnalyzer

v6.2+



FortiSIEM


v5.0+

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response


Services that can automatically respond to this outbreak.



FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.




Incident Response

RECOVER

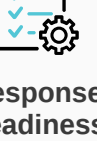
Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.




NSE Training



Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.




Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.




Security Rating

Additional Resources

| | |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Helpnet Security | https://www.helpnetsecurity.com/2023/01/17/cve-2022-47966-poc/ |
| Bleeping Computer | https://www.bleepingcomputer.com/news/security/cisa-warns-of-critical-manageengine-rce-bug-exploited-in-attacks/ |
| The Hacker News | https://thehackernews.com/2023/02/experts-sound-alarm-over-growing.html |
| Bleeping Computer | https://www.bleepingcomputer.com/news/security/f5-urges-customers-to-patch-critical-big-ip-pre-auth-rce-bug/ |
| Threat Post | https://threatpost.com/f5-critical-bugbig-ip-systems/179514/ |
| Threat Signal | https://www.fortiguard.com/threat-signal-report/3891 |

Learn more about [FortiGuard Outbreak Alerts](#)

 FortiGuard Labs

FORTINET